CLAIMS

We claim:

1. A computer-implemented method for providing access to an information account stored in a central data repository that is accessible via a distributed network, the information account containing consumer information elements that can be altered by the consumer, the method comprising the steps of:

receiving, over the distributed electronic network, a first request from a network device for access to the information account and consumer authentication information in response to the consumer inputting the consumer authentication information while interacting with a first web-site;

in response to the request, authenticating the consumer based on the consumer authentication information, thereby providing the consumer with access to the information account; and

in response to authenticating the consumer, automatically managing subsequent authentications of the consumer so that the consumer will not be required to again input the consumer authentication information upon initiating a second request for access to the information account while interacting with a subsequent web-site that is configured to provide access to the information account upon authentication of the consumer.

2. A computer readable medium having stored thereon computer executable instructions for performing the method of claim 1.

3. The method of claim 1, wherein automatically managing subsequent authentications of the consumer comprises determining that a previous authentication of the consumer for access to the information account remains valid and generating a message to cause the subsequent web-site to by-pass a sign-on interface that would otherwise prompt the consumer to input the consumer authentication information when the consumer initiates the second request for access to the information account.

4. A computer readable medium having stored thereon computer executable instructions for performing the method of claim 3.

5. The method of claim 3, wherein the previous authentication of the consumer remains valid if the consumer initiates the second request for access to the information account prior to the occurrence of a terminating event.

6. The method of claim 5, wherein said terminating event comprises expiration of a time-out interval.

7. The method of claim 6, wherein the time-out interval comprises a determined duration of time; and

wherein the time-out interval is considered to have expired if a difference between a current time and a time of the previous authentication is greater than the determined duration of time.

8. The method of claim 5, wherein said terminating event comprises termination of a browser session at the network device.

9. The method of claim 1, wherein the network device comprises a client device executing a browser; and

wherein the single sign-on function is implemented by one or more temporary client-side applications.

10. The method of claim 9, wherein said one or more client-side applications execute a communication protocol for communicating with a database management system at a host server that manages the central data repository.

11. The method of claim 9, wherein the network device executes a browser that displays a web page file that has been retrieved from a vendor server, the web page file including an instruction that causes the browser to request transmission of said one or more client-side applications.

12. The method of claim 9, wherein said one or more client-side applications are further configured to receive selected consumer information elements from the information account in response to authentication of the consumer and to

integrate the consumer information elements into a vendor's business process on behalf of the consumer.

13. The method of claim 12, wherein the step of integrating the selected consumer information elements into a vendor's business process comprises the steps of:

auto-populating the selected consumer information elements into at least one input field of a web page file that has been received from a vendor server; and

allowing the consumer to interact with the browser in order to edit the selected consumer information elements, if desired, and to submit the web page file to the vendor server for processing of the selected consumer information elements.

14. A computer readable medium having stored thereon computer executable instructions for performing the method of claim 13.

15. The method of claim 1, wherein the information account comprises a plurality of consumer information elements stored in a tagged data format.

16. The method of claim 1, further comprising receiving from the network device a first-determined equipment identifier that uniquely identifies the network device and storing the first-determined equipment identifier in an authentication table in association with the consumer authentication information; and

wherein automatically managing subsequent authentications of the consumer comprises recording in the authentication table in association with the consumer authentication information and the first-determined equipment identifier an indication that a single sign-on feature is activated.

17. The method of claim 16, further comprising the steps of:

receiving from the network device a second-determined equipment identifier in response to the consumer initiating a second request for access to the information account;

in response to receiving the second-determined equipment identifier, consulting the authentication table based on the second-determined equipment identifier and determining that the second-determined equipment identifier matches the first-determined equipment identifier;

based on the first-determined equipment identifier, determining from the authentication table that the single sign-on feature is activated; and

transmitting to the network device a message to cause a sign-on interface that would prompt the consumer to input the consumer authentication information to be by-passed.

18. A computer readable medium having stored thereon computer executable instructions for performing the method of claim 17.

19. The method of claim 17, wherein automatically managing subsequent authentications of the consumer further comprises:

recording in the authentication table in association with the consumer authentication information and the first-determined equipment identifier, a time at which the consumer was authenticated to access the information account;

in response to determining that the single sign-on feature is activated, determining from the authentication table the time at which the consumer was authenticated; and

prior to transmitting the message to by-pass the sign-on interface, determining that a difference between a current time and the time at which the consumer was authenticated is not less than a time out interval.

20. A computer readable medium having stored thereon computer executable instructions for performing the method of claim 19.

21. The method of claim 1, wherein automatically managing subsequent authentications of the consumer is performed in response to an input command supplied by the consumer to indicate that a single sign-on feature should be activated.

22. A computer-implemented method for accessing an information account stored in a central data repository that is accessible via a distributed network, the information account containing consumer information elements that can be altered by the consumer, the method comprising the steps of:

transmitting to a host server, over the distributed electronic network, a first request for access to the information account and consumer authentication information in response to the consumer inputting the consumer authentication information while interacting with a first web-site hosted by a vendor server;

receiving an acknowledgment indicating that the host server authenticated the consumer based on the consumer authentication information, thereby providing the consumer with access to the information account; and

in response to the acknowledgment, automatically managing subsequent authentications of the consumer so that the consumer will not be required to again input the consumer authentication information upon initiating a second request for access to the information account while interacting with a subsequent web-site that is configured to provide access to the information account upon authentication of the consumer.

23. A computer readable medium having stored thereon computer executable instructions for performing the method of claim 22.

24. The method of claim 22, wherein the consumer interacts with the first web-site using a browser;

wherein the first web-site includes an instruction that causes the browser to download from the host server one or more client-side applications configured for automatically managing subsequent authentications of the consumer.

25. The method of claim 24, wherein the one or more client-side applications are configured to perform the steps comprising:

determining a plurality of selected consumer information elements that are to be input into input fields of the first web-site;

transmit to the host server a request for retrieval of the selected consumer information elements; and

in response to receiving the selected consumer information elements from the host server, auto-populating the selected consumer information elements into the input fields of the first web-site.

26. A computer readable medium having stored thereon computer executable instructions for performing the method of claim 25.

27. The method of claim 22, wherein the consumer interacts with the first web-site using a network device; and

wherein automatically managing subsequent authentications of the consumer comprises:

determining a first-determined equipment identifier that uniquely identifies the network device and transmitting the first-determined equipment identifier to the host server for storage in an authentication table in association with the consumer authentication information,

in response to the consumer initiating a second request for access to the information account, determining a second-determined equipment identifier and transmitting the second-determined equipment identifier to the host server, wherein the host server consults the authentication table based on the second-determined equipment identifier to determine that the second-determined equipment identifier matches the first-determined equipment identifier and, by association, that the consumer has previously been authenticated and that a single sign-on feature is activated, and

receiving from the host server a message to cause the subsequent web-site to by-pass a sign-on interface that would otherwise prompt the consumer to input the consumer authentication information.

28. A computer readable medium having stored thereon computer executable instructions for performing the method of claim 27.

29. The method of claim 22, wherein the step of automatically managing subsequent authentications of the consumer is performed in response to detecting an input command supplied by the consumer to indicate that a single sign-on feature should be activated.

30. The method of claim 22, wherein automatically managing subsequent authentications of the consumer comprises communicating with the host server to determine that a previous authentication of the consumer for access to the information account remains valid and to instruct the subsequent web-site to by-pass a sign-on interface that would prompt the consumer to input the consumer authentication information when the consumer initiates the second request for access to the information account.

31. The method of claim 30, wherein the previous authentication of the consumer remains valid if the consumer initiates the second request for access to the information account prior to the occurrence of a terminating event.

32. The method of claim 31, wherein said terminating event comprises expiration of a time-out interval.

33. The method of claim 32, wherein the time-out interval comprises a determined duration of time; and

wherein the time-out interval is considered to have expired if a difference between a current time and a time of the previous authentication is greater than the determined duration of time.

34. The method of claim 31, wherein said terminating event comprises termination of a browser session.

35. A system storing, managing and distributing consumer information via a distributed network, comprising:

a central data repository accessible via the distributed electronic network for storing an information account, the information account containing consumer information elements that can be altered by the consumer; and

a host server for communicating with the central data repository and with a network device via the distributed electronic network and for executing computer-executable instructions for:

receiving, over the distributed electronic network, a first request from the network device for access to the information account and consumer authentication information in response to the consumer manually inputting the consumer authentication information while interacting with a first web-site;

in response to the request, authenticating the consumer based on the consumer authentication information, thereby providing the consumer with access to the information account; and

in response to authenticating the consumer, automatically managing subsequent authentications of the consumer so that the consumer will not be required to again input the consumer authentication information upon initiating a second request for access to the information account while interacting with a subsequent web-site that is configured to provide access to the information account upon authentication of the consumer.

36. The system of claim 35, wherein automatically managing subsequent authentications of the consumer comprises determining that a previous authentication of the consumer for access to the information account remains valid and generating a message to cause the subsequent web-site to by-pass a sign-on interface that would otherwise prompt the consumer to input the consumer authentication information when the consumer initiates the second request for access to the information account.

37. The system of claim 36, wherein the previous authentication of the consumer remains valid if the consumer initiates the second request for access to the information account prior to the occurrence of a terminating event.

38. The system of claim 37, wherein said terminating event comprises expiration of a time-out interval.

39. The system of claim 38, wherein the time-out interval comprises a determined duration of time; and

wherein the time-out interval is considered to have expired if a difference between a current time and a time of the previous authentication is greater than the determined duration of time.

40. The system of claim 37, wherein said terminating event comprises termination of a browser session at the network device.

41. The system of claim 35, wherein the network device comprises a client device executing a browser;

wherein the host server further comprises a memory for storing one or more client-side applications configured to manage communications with the host server and to automatically manage subsequent authentications of the consumer on behalf of the client device; and

wherein the host server executes further computer-executable instructions for transmitting to the client device said one or more client-side applications prior to receiving the first request for access to the information account.

42. The system of claim 41, wherein the browser displays a web page file that has been retrieved from a vendor server, the web page file including an instruction that causes the browser to request transmission of said one or more client-side applications from the host server.

43. The system of claim 35, wherein the information account comprises a plurality of consumer information elements stored in a tagged data format.

44. The system of claim 35, wherein the host server further executes computer-executable instructions for:

receiving from the network device a first-determined equipment identifier that uniquely identifies the network device and storing the first-determined equipment

identifier in an authentication table in association with the consumer authentication information; and

wherein automatically managing subsequent authentications of the consumer comprises recording in the authentication table in association with the consumer authentication information and the first-determined equipment identifier an indication that the single sign-on function is activated.

45. The system of claim 44, wherein automatically managing subsequent authentications of the consumer further comprises:

receiving from the network device a second-determined equipment identifier in response to the consumer initiating a second request for access to the information account;

in response to receiving the second-determined equipment identifier, consulting the authentication table based on the second-determined equipment identifier and determining that the second-determined equipment identifier matches the first-determined equipment identifier;

based on the first-determined equipment identifier, determining from the authentication table that the single sign-on function is activated; and

transmitting to the network device a message to cause a sign-on interface that would prompt the consumer to input the consumer authentication information to be by-passed.

46. The system of claim 45, wherein automatically managing subsequent authentications of the consumer further comprises:

recording in the authentication table in association with the consumer authentication information and the first-determined equipment identifier, a time at which the consumer was authenticated to access the information account;

in response to determining that the single sign-on function is activated, determining from the authentication table the time at which the consumer was authenticated; and

prior to transmitting the message to by-pass the sign-on interface, determining that a difference between a current time and the time at which the consumer was authenticated is not less than a time out interval.

47. In or for a system for providing access to an information account stored in a central data repository that is accessible via a distributed network, the information account containing consumer information elements that can be altered by the consumer, a propagated signal carrying thereon a data structure comprising:

a client-side application configured for automatically managing authentication of the consumer at a network device so that the consumer will not be required to input the consumer authentication information upon initiating a request for access to the information account while interacting with a web-site that is configured to provide access to the information account upon authentication of the consumer;

wherein the client-side application automatically manages authentication of the consumer by communicating with a host server to determine that a previous authentication of the consumer providing the consumer with access to the information account remains valid and to instruct the web-site to by-pass a sign-on interface that would otherwise prompt the consumer to input the consumer authentication information when the consumer initiates the request for access to the information account.

48. The propagated signal of claim 47, wherein the previous authentication of the consumer remains valid if the consumer initiates the second request for access to the information account prior to the occurrence of a terminating event.

49. The propagated signal of claim 48, wherein said terminating event comprises expiration of a time-out interval.

50. The propagated signal of claim 49, wherein the time-out interval comprises a determined duration of time; and

wherein the time-out interval is considered to have expired if a difference between a current time and a time of the previous authentication is greater than the determined duration of time.

51. The propagated signal of claim 48, wherein said terminating event comprises termination of a browser session at the network device.

52. The propagated signal of claim 47, wherein the client-side application is configured for determining an equipment identifier that uniquely identifies the network device and transmitting the equipment identifier to the host server;

wherein, in response to receiving the equipment identifier, the host server determines that the previous authentication of the consumer remains valid by consulting an authentication table to determine that the equipment identifier matches a previously-stored equipment identifier, that an indication that a single sign-on feature is activated is stored in association with the previously-stored equipment identifier and that a terminating event has not occurred; and

wherein, in response to determining that the previous authentication of the consumer remains valid, the host server transmits to the client-side application a message to cause the web-site to by-pass a sign-on interface that would prompt the consumer to input the consumer authentication information.

53. The propagated signal of claim 52, wherein the client-side application is further configured to receive selected consumer information elements from the information account in response to authentication of the consumer and to integrate the consumer information elements into a vendor's business process on behalf of the consumer.

54. The propagated signal of claim 53, wherein integrating the selected consumer information elements into a vendor's business process comprises the steps of:

auto-populating the selected consumer information elements into at least one input field of a web page file received from a vendor server; and

allowing the consumer to interact with the browser in order to edit the selected consumer information elements, if desired, and to submit the web page file to the vendor server for processing of the selected consumer information elements.

55. The propagated signal of claim 47, wherein the information account comprises a plurality of consumer information elements stored in a tagged data format.